Growing dependency on IT
(The consequences thereof for the organization and for IT-auditors)

Prof. Margaret E. van Biene-Hershey RE
Vrije University
Boolelaan 1105, 1081 HV Amsterdam, the Netherlands
Tel: 31(0)348 44 4387   Fax: 31(0)348 44 3971
E-mail: rj.van.biene@accountnet.nl

1 INTRODUCTION

This article presents a general outline of the effects of the use of information technology in companies. The picture that emerges will show when and why IT-auditing became necessary as a profession and the reasons why the necessity is destined to become even greater in the future.

First, the changing position of information technology within the economy is sketched in broad terms; after that the position is shown of information systems within the corporate economy of the future. Some salient points are mentioned for consideration in relation to security, continuity and reliability in this future picture. And finally, in the summary, certain myths are disposed of concerning the control mechanisms required for electronic processes and the challenges are described facing companies and IT-auditors.

The subjects discussed in this article all concern the consequences of using computers for organizations in general; particular typologies are not elaborated.

When a company has been automated to the point where its activities are recorded with no significant human intervention, then a situation may be said to have arisen in which the computer acts as a partner in the execution of corporate activities. Organizations that make use of all the forms of computer support described below for their company's processes may be classed as automated to the extent that the computer has become a partner in the execution of corporate activities:

S. Jajodia et al. (eds.), *Integrity and Internal Control in Information Systems*

- Orders for services and/or products are received by the organization by electronic means;
- Warehousing is entirely managed by computer controlled robots;
- Manufacturing processes are computer controlled;
- All financial transactions with banks, suppliers and customers are completely automated;
- Management tasks are fully supported by information supplied nearly exclusively by means of electronic processes.

Such full 'partnership' has not yet been achieved. But it is already an important point of management policy at present and will be even more so in future, because there are a number of extremely important advantages inherent in this situation. Processes are carried out more cheaply and reliably in this way than when they are performed by people. Further on in this article we will examine the reasoning underlying this statement. People will be carrying out activities that are more interesting than the routine tasks associated with executing basic processes day by day, and they will attach greater importance to the (needs of the) company's clients.

There are a number of fundamental reasons, quite apart from specific company typology, why this 'partnership' with automation leads to an organizational structure that is quite different from that arising from a situation in which the tasks concerned are carried out by human agency. For instance, computers are not capable of self-seeking behavior. Processes that have been automated may be regarded as 'systematic'. This means that, given identical input, and if the conditions of execution are always constant and the same basic files are used, these systems should, barring unforeseen circumstances, yield identical results. In the case of systematically automated processes it is thus important to ensure that organizational conditions are such that processes will do what they are supposed to do and that their execution will take place undisturbed.

This 'partnership' between man and the computer is a natural development in the use of computers in our society. It is a development that can also be shown from the perspective of internal audit and security. For this reason, we have summarized the effects of automation on control structures and security measures within the organization in the past, before turning our attention to the specific features of the consequences of using the computer as a partner in business management.

2 ROLE OF KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGIES IN THE CORPORATE ORGANIZATION

If the past may be characterized by use of the word 'mechanization' and the present by 'automation', the watchword for the future is 'knowledge management'. The term 'knowledge management', in particular, is probably used here in a slightly different sense from usual, while our use of the term 'automation' may be doing less than justice to the current position. However, the usual meaning attached to these terms covers about 70% of the interpretation given in this article. Suggestions for better terminology are most welcome. A time scale for the three phases in given in Figure 1.

Thus, three phases are distinguished, namely:

- **Mechanization:** the computer takes over certain tasks from people without affecting the structure of the organization or the way people work; the computer clearly plays a supporting role;
- **Automation:** the way people work is reorganized in such a way that important tasks and even entire jobs are carried out by computer;
- **Knowledge management:** the jobs are carried out or even directed by computers, people support the computerized tasks and the computer is a partner in operational management.

In the rest of this chapter we will examine the most important characteristics of internal control and security in these three phases in the use of computers within companies.

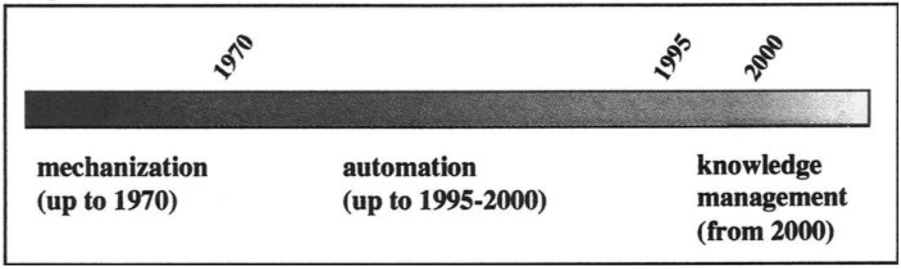

Figure 1: Time scale for phases in use of IT

2.1 Mechanization

The use of computers in industry in support of human tasks was necessary to achieve the requisite degree of efficiency and accuracy in operational management. The connection between computer support and human corporate activity was that at set intervals people had to prepare the results of their labors for processing by a computer. At other set times, they had to be in a position to take delivery of output from a computer, to assess it and to make use of it in carrying out their tasks. Processing was usually by batch processes and if any inaccuracies emerged, it was possible simply to repeat the process. If there was a certain critical time element, it was usually a matter of hours rather than minutes. Although it was generally acknowledged that automated execution was more accurate (more reliable) and faster (more efficient) than was feasible in an exclusively human organization, people did not trust the computer to be sufficiently systematic or of sufficient integrity to render checking the results of the process unnecessary.

During this generation of computer use, all activities (i.e. all output) were checked for completeness and accuracy before the results of the process affected operational management.

Controlling the processing usually included integrity controls on the input and output of the computer center, while controls on the completeness and on accuracy aspects were not always carried out by the same organizational units. Checks of the accuracy of the input were carried out by those responsible for input, and checks were carried out by the computer center before processing began to check on the completeness of the input data. The computer center checked the accuracy and completeness of the processing before the output was dispatched to the user. Employees in the business department concerned checked the accuracy of the results of the process. The department to some extent also checked the completeness of the processing and then, preferably by someone other than the person who had checked the output. The systems were developed by professional developers who were responsible for adequate testing and implementation of the programs on a production computer (or for transferring these to the change management department and computer operators).

There were no great inherent risks attached to this way of doing things because the user checked all input reports and the computer's output for accuracy. All output, moreover, was controlled for completeness. If any omissions were picked up, these were the fault of the computer center for not checking the completeness of the input data sufficiently thoroughly before the production processes started. The interdependence of the various production processes was managed by checking that all input data was present, before processing started.

So long as computer centers were using tapes and punch cards, the operation formed an easily manageable whole. The introduction of disc units made it necessary to create guarantees within the organization of the computer center to make it possible to ascertain that the data on the disc units remained unchanged during the intervals between the various production processes.

The ledger and networks of check sums maintained by personnel gave the company early insight into the completeness and accuracy of the management of the company as a whole.

2.2 Automation

With automation, the first steps were taken towards further integration of the organization of tasks and the use of computerized processes. This led to the integration of the computer in the workplace, initially by using 'dumb' terminals and later personal computers. Human beings initiated transactions that were processed partly on their own personal computers and partly on a (more) centrally managed computer system. Operational management was organized in such a way that use of the computer was maximized. The clear distinction between input, processing and output, which all had their own specific check phases, disappeared. The promptness of automated support was perceived as the degree to which the response times of such support varied within agreed limits. These limits were defined as a particular percentage of the response time and were (and are) expressed in terms of a few seconds.

This new way of processing data posed new problems for controlling and general manageability. The continuity (availability and response times) of automated support requires measures specifically designed for this new situation. These measures are carried out largely within the technical infrastructure and in the procedures of the computer center and the arrangements made with it, and not in the information systems and the organization of the users. In order to achieve the requisite accuracy in its processing results, the organization inevitably becomes dependent on the checking procedures within the system. This leads to a stricter control on process integrity, rather than a control on data integrity. Such controls on process integrity are carried out by means of extensive tests and acceptance procedures when new or modified systems are installed. The accuracy of the data is checked by the manner in which transactions are processed by the integrity of the automated processes. The authorization to introduce transactions must be preventatively controlled in order to prevent inaccurate processes. As a consequence of this issue, the integrity of the technical infrastructure must also be guaranteed. The method of processing often leads to individuals having authority delegated to them so that they can use the computer to carry out independent processing: this means that the tasks carried out are not checked by a second member of staff. To perform checks, the applications are equipped with all possible relational controls, and individual authorizations are determined and entered into the automated systems so that the automated systems can check them. The completeness of the processing cannot be determined simply. Networks of check sums that are separate from the automated system often do not operate promptly enough; furthermore, these networks are often ineffective due to the processing volume. In order to be able to rely on automated networks of check sums, reliable automated operation of several processes that are independently organized and used is required. In other words, the implementation of automated systems must take place in reliable environments.

The organization controls the automated system and no longer directly controls the individual processing of specific input and the resulting specific output. The checks which, in combination, have to determine the integrity of processing are of a very preventative nature. The professional developer must supply systems that are explicitly tested and accepted by a user: the user must test that all the checks needed are present. Production is done separately from the development of systems, so that no unauthorized changes can take place in the production systems. The organization monitors the integrity of the change processes with respect to changes in the production environment. There is a form of access control that limits the access of all those involved in the organization (including the computer center personnel) to those functions for which they are authorized. There is also an explicit control on the access to and use of data by employees. The delegation of responsibility to use transactions and the limited functionality of the transactions are both designed to lead to a constant presence of inevitable conflicts of interest among the staff concerned. These conflicts of interest can also lead to retrospective opportunities to check the accuracy of the processing (networks of check sums). Where necessary, a risk analysis can result in transactions only being processed after explicit approval is given by an employee with the authority to do so. A distinction is made between transactions that are critical for the organization and other transactions that are not considered critical. The critical transactions are provided with meticulous preventative controlling measures within and through the automated systems, to prevent misuse and/or inaccurate results. The computer center uses a variety of automated processes that monitor the integrity of the process sequence. The completeness of the processing is checked using specially designed processes, which operate alongside transaction processing, or are run after the business processing has been completed.

The organization can test whether the results of automated processing are complete and accurate. However, such tests require a strict control of the system of the automated processes and of the management of these processes. In order to determine that the organization has the requisite technical infrastructure available and is managing its information systems properly, an auditor must have explicit knowledge of automation techniques and of the relationship between automated processes. The professional IT-auditor has become necessary.

2.3 Knowledge management

Automated processes are becoming more and more intelligent. People are no longer able to verity the processing results. People accept that the results of the processing as complete and accurate, without additional control measures. The company employee no longer has to 'feed' the computer with transactions and check whether the processing is complete and accurate. The human being within the company is free to perform more effective tasks. He or she is then concerned with activities such as providing services to others, selling services (often computer controlled services), purchasing raw materials, selling products, using information supplied by the computer, assessing irregularities and solving 'problems' indicated by the computer.

The data to be processed are entered 'automatically' outside the company, in warehouses or by production machinery. It is not possible to verify the accuracy of this input, because it fed directly to the automated systems. In particular, the responsibility for its accuracy and completeness lies with an external third party, or the input is obviously accurate precisely because it is generated as an integral part of the manufacturing process. The output resulting from the processing leaves the company again, or controls production machinery without human intervention.

The differences from the previous phase as described in paragraph 2.2, and also the possible problems, are mainly associated with the required continuity of computerized support and the even more urgent need for preventative controls on the running of the processes. Systems must be continuously available to ensure smooth operations. It is not possible for employees within the organization to check the accuracy and completeness of the individual data supplied. The computer checks the relations between processes and systems and reports irregularities to the employees within the company. Completeness of the processing is ensured by the fact that everything which is supplied is also (one way or another) processed.

The system controls its own processing completeness and sends messages to the human agent to resolve discrepancies, so that the system can guarantee the required continuous completeness. The whole organization of the process is set up in such a way that access authorization and the required recording of communication between systems and between the system and the human agent is completely regulated. The problems with respect to the retrospective checks on the operating processes are the same as those described in paragraph 2.2.

All control procedures are of a preventative nature, with the exception of those measures that serve to determine that the preventative checking procedures have worked. All repressive control procedures are, however, also computerized. Man has adaptive controls at his disposal (facilities to direct the control procedures). These 'human interventions' are mainly activated using the management information made available to management and the analyses performed by man of possible systematic causes of requests generated by the computerized system to solve problems indicated. External factors can also induce management to introduce changes in processing parameters or in the process itself.

The resources available today make it possible to organize knowledge management so as to guarantee reliable and complete management information. The design of the computerized system is then such that the organization can rely on the computerized processes on which these demands are made to run with integrity on a continuous basis. The processes can be regarded as reliable because they have integrity (adequate test and acceptance procedures, all changes in systems are tested and approved). The input is, by definition, correct (the inputting bodies take the responsibility for this). The control tables etc. as well as all data have integrity by definition (plausibility checks, limited human intervention). The operational output and the data stored in computerized form have integrity (because the processing has). The (possibly necessary) processes for extracting data for management information have integrity (the same conditions apply to this as all other processes), as does the control information for the refinement process (the same grounds apply as for the other control tables). The management can request information from the computerized systems without negatively influencing the reliability of the systems, and the management is familiar with the procedures designed for this. In this way, management is provided with reliable information.

The (alarming) result of this kind of knowledge management is that middle management has become superfluous. Top managers can identify their own information needs and obtain the desired information simply and without endangering the reliability of the basic processes.

When in importance of the technical support of the business processes is not fully appreciated, there will be organizations that believe that 'knowledge management' has no special effect on the way auditing needs to be carried out. They will think that they can continue to audit responsibly as has been described in section 2.2, without technical IT-auditing. However, when knowledge management takes the form described in this section, companies will be forced to recognize that independent and impartial experts must be asked to judge the adequacy of the technical organization of the computer systems. This means an explicit assessment of the technical infrastructures and the organizations that design, implement and perform maintenance on these technical systems. Completeness of the control procedures in the technical environment and in the information systems, as well as the links between the two, is of vital importance to organizations.

The measures needed to be able to use computers in this way are described in the following section.

3 CONDITIONS FOR KNOWLEDGE MANAGEMENT

Although from the point of view of 'knowledge management' the computer is clearly seen as a partner in the organization of the company and not merely as support to human operation, the computer must also play a supporting role in the tasks which still have to be done by man. For this reason, before dealing with the facilities needed in IT organization, some conditions will be discussed which refer to the delegation of responsibility to the various company employees. The subsequently discussed facilities in the IT systems organization will be handled on three levels:

- Technical infrastructure;
- Structuring information systems;
- User organization.

Naturally, the totality of measures on the three levels must be consistent and efficient. This means that the segregation of duties required within the organization must be completely safeguarded in the structure of the information systems and in the technical infrastructure. When the same technical structure or the same information system supports several deliberately separated parts of the organization, it must meet particular requirements. This also applies to the IT organization described in section 2.2.

The architecture of the cooperating computerized processes must make it possible for the computer to carry out the required detective controls independently. The computer is not self-seeking, and therefore the structure of computerized administrative procedures should not, in theory, need any modularity or interfaces. Later in this section we will show that the requirements of controllability mean that it is necessary to divide up processes in such a way that the computer can guarantee uniform processing.

3.1 Authorization

Authorization means the delegation of responsibility. As such, it is the technique that is used to effect the desired segregation of duties within the organization. Authorization is, consequently, a function that only occurs in situations where people are working together. Computers cannot delegate; even where there is partnership between man and computer. Maybe a subsequent evolutionary step will lead to the computer's powers being so superior to human ability that they will be able to manage people better than we ourselves can. In this situation, the computer could possibly perform the authorization function.

The authorization specifications laid down by an organization are entered into the computer, which checks that people (can) only get access to the resources for which they are authorized. This is termed ‘access control’. Naturally, the computer must be able to determine the identity of the employee concerned (authenticating the identity entered, if necessary using 'identity proofs').

Segregation of duties is applied first and foremost to limit the risks associated with delegating responsibilities to employees. This means that duties must be segregated both vertically and horizontally.

Vertical segregation of duties limits the authority of staff members in relation to the structure and the design of computerized processing. The employee's responsibilities are determined in such a way that it is not possible for him or her to manipulate the links between computerized processes or to influence them in any other way so as to damage the interests of the organization. Introducing adequate vertical segregation of duties should result in the creation of access specifications, which can be entered into the computer so that access to computer programs and files can be restricted and monitored.

Horizontal segregation of duties limits the financial powers of an employee's area of responsibility. This segregation of duties and the procedural consequences for the computerized systems should also be fully computerized. This will not be regulated by access control software only, but also by controls and procedures, which are built into the computerized administrative processes.

When defining the segregation of duties, the organization must take into account the fact that the computer has become a partner in the organization of the performance of duties, and that man no longer has the opportunity to intervene at an appropriate time in computerized processes. The input supplied for processing will be checked by the system, but no longer on the initiative of man or by man. Man will, of course, take action when the system refuses input and refers it back to the human organization for correction. However, these referrals will be highly exceptional.

3.2 Technical infrastructure

It must be clear that not every use of automation will have to meet strict control and security requirements. The efficiency and effectiveness of the work carried out by the various employees of the company will, to a great extent, be determined by the technical infrastructure of the computerized systems. In order to prevent all computerized systems from being subject to one single regime of control, IT environments are distinguished which are sufficient for the different levels of control and security. The way in which the levels are technically separated depends on the differences in the required control and security typologies of the various environments. The differences arise from an analysis of the actual risks to the organization of the various classes of business information and processes. The first requirement for this level of IT support is therefore the management of the IT infrastructure in accordance with a classification into separate environments which are derived from a risk analysis and a well considered decision process for general control and security procedures for each separate environment.

The actual access control therefore does not only require detailed consideration of the consequences of the employees' authorities in terms of access to data and processes, but also of the design of the links between separate environments so that no unacceptable risks arise of undesired communication between these environments. The role of the current access control software will be limited to the initial procedure for identifying the user and access monitoring for an IT environment. Within an environment, if necessary, the database management system will perform the most important monitoring of the access to data and processes (object monitoring).

From a technical point of view, every environment will be regarded as an 'open shop environment' or as a 'closed shop environment'. Most environments should be classified as 'open shop' with varying degrees of controls on, firstly, the manner in which access is obtained, and, secondly, on the processes available in the specific environment. In open shop environments control will still be possible to varying degrees. These controls will check:

- Integrity of the logging of computerized processes;
- Destination of the output;
- Security of the typology of the linked systems;
- Identification of users;
- Integrity of processes and data;
- Continuity of processes and data;
- Opportunities for making changes in the processes and the technical infrastructure.

In a closed shop environment there will be guarantees concerning:

- Integrity of the logging of computerized processes;
- Integrity of the input and the processes;
- Integrity of the technical infrastructure;
- Scopes of responsibilities of explicitly identifiable users;
- Desired continuity and availability of data and processes;
- Integrity of all changes in processes and in the technical infrastructure.

The destination of the output in a closed shop environment is not a specific point for attention because the technical infrastructure, the processes and the data guarantee the correct destination.

The closed shop is the only environment suitable for applications in which the control structure is so extensive that even the repressive measures are computerized. The remainder of this article deals exclusively with the closed shop environment.

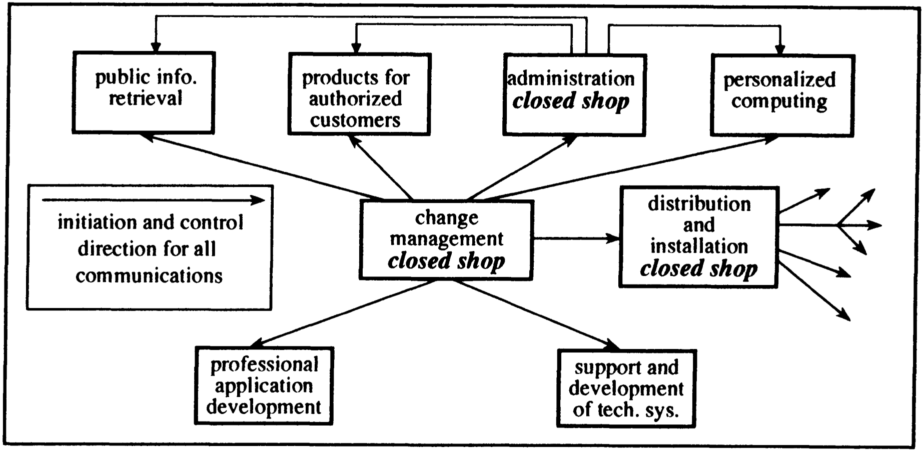
public info. retrieval
products for authorized customers
administration
closed shop
personalized computing
initiation and control direction for all communications
change management
closed shop
distribution and installation
closed shop
professional application development
support and development of tech. sys.

Figure 2: Strategy for distinguishing environments for information systems with common security requirements

3.3 Structuring information systems

As stated earlier, consistency between the segregation of duties in the organization and the architecture of the supporting information systems is extremely important. This segregation across different IT environments can mean that the information system is designed in such a way that different parts of the total process run in different open and closed shop IT environments according to their required security levels for processing.

An automatic check is carried out into the completeness and accuracy of the results of the processes per source of activities, before going on to those procedures which lead to the critical processes executed in the closed shop environment and which lead in turn to deliveries and payments. The precondition for automating detective and repressive control measures is that the structure of the automated processes must lend itself to the establishment of controlled links between IT environments. For this reason, the modularity and the interfaces between modules must be designed so that the detective and repressive controls can be based on these. To achieve this, each type of source (and therefore also the link between the computers) must in itself have its own recognizable position in the architecture. Names of specific sources and destinations will be unique within the internal organization as a whole (banks, suppliers, purchasers etc.). Communication links which are needed to meet obligations laid down by the authorities (e.g. VAT return), possible external supporting bodies and external information sources will be included in the architecture in such a way that the closed shop characteristics of particular environments are never affected by these links.

There are processes in the critical closed shop environment, which generate forecasts relating to important parameters in the context of the movement of money and goods. These computer generated forecasts are used, at predefined moments in the processing, to carry out a completeness check before determining that conclusions can be drawn on the basis of the processes concerned.

There are limits to the scope of all processes, depending on the classification of the process and the control specific consequences associated with the environment in which the process is carried out. The processes in a closed shop environment, by definition, have control and security procedures of such a quality that it is possible to check the completeness and the accuracy of the processes and their results in an open shop environment. The designed interfaces with the open shop environment are technically sufficient for this. The open shop environment cannot negatively influence the closed shop environment.

Although the information systems' control structures must be consistent with the company's policy, the architecture of the information system is not dependent on the organizational structure within which the users of the information systems happen to be working. The architecture of the computerized information systems is designed to guarantee the internal integrity of the processes. Access control technologies monitor the segregation of duties in the user organization and the access to the computer by external bodies.

3.4 User organization

The users of IT systems are:

- Computer center staff;
- Professional system developers;
- System programmers;
- System engineers;
- Business staff;
- Other staff;
- Manufacturing processes;
- Computers not belonging to the legal entity.

This list provides a starting point for deciding on the most important environments to be differentiated. The remainder of this section confines itself to the issue of the relationship between this list of users and the closed shop environment and the controllability of company operations.

The **computer center staff** will not have direct access to the closed shop environment. Should the closed shop environment experience technical problems that require human intervention or should the resources available to the environment need to be up or down graded then computer center staff will have momentary authorization to interact with the closed shop environment. Examples of situations include process or data structure reorganizations, introduction of new hardware, changing system parameters to allow safe preventative hardware maintenance.

In other words, the system and process monitoring are completely automated. The conditions for 'real time' back up will be created on an ongoing basis by the system itself, and, in an emergency, the system will automatically switch over to the backup system.

Professional system developers do not have access to closed shop environments. If troubleshooting is needed, all the necessary data and copies of processes are dumped on systems where the professional developer can make the necessary changes on the basis of analyses performed. The professional developer may be authorized to consult the closed shop environment during the troubleshooting. However, changes to the systems will only be entered in the closed shop environment after a second developer has explicitly checked the changes, the changes have been approved by the owner of the system and by the computer center. Hopefully there will be procedures that provide forecasts of the relationship between the cause, or the reason for the change, and the effect of the change so that an analysis can be made as to whether only required code changes have been introduced.

Technical system managers (**system programmers** and/or **system engineers**) never have access to closed shop environments. System software is introduced into the production environment via a route guaranteeing optimum stability and reliability before the software becomes operational in the closed shop environment.

In many cases, **business staff** is authorized to consult the environment to call up predefined standard output (i.e. no ad hoc 'query facilities'). There may be corporate staff members who are responsible for certain adaptive controls of the system and who can therefore alter certain very critical tables or data sets. It goes without saying that such a responsibility must be implemented in such a way that employees can be identified precisely enough for them to be subsequently called to account for their actions. It is also possible to design a procedure for interaction so that two employees are responsible for the accuracy of the input.

Other staff will not have access to the closed shop environment but they will have access to other open shop environments. The closed shop environment will take the data needed for the closed shop processes from the open shop environments in a safe and controlled way. Employees and other computers (internal or external to the organization) requesting free information will not have any access to the closed shop environment.

Machines for **manufacturing processes** will, where necessary, have their own closed shop environments which are separate from the administrative closed shop environment because the automated systems for production will set higher continuity and response time requirements than are necessary for the administrative environment.

The **computers not belonging to the legal entity** (for example: clients, consumers, government and banks) will not have direct links with the closed shop environment.

This article may create the impression that the concept of human control has disappeared entirely from the internal organization. This is not the case. There are circumstances in the organization of the business activities will make a 'back office' necessary. This situation arises whenever there are functions in the internal organization for which no effective segregation of duties can be created and the materiality of an action cannot be limited with automated tools. The organization will then have to delay processing the results of the performance of these functions and actions by maintaining a second function in the company which checks the actions of those which performed the first function in a timely manner. This check is geared to the extent to which the functions are performed within the policy guidelines of the company. Those performing the check are authorized to take action in good time to limit the consequences of misappropriation. An example of the situation alluded to here is the purchase and sale of cash, where such purchase and sale occurs in the first instance through agreements between people. These agreements must then be recorded in the system preferably by means of an action performed by another person, independently of the agreement. If the computer can derive the agreements from a conversation, it is conceivable that the computer might be able to intervene to prevent unauthorized agreements being made. This will be conceivable when voice recognition becomes sufficiently sophisticated.

Employees will have to be available in the human organization who can be directed by the computer to solve technical problems with which the computer cannot cope. These people contribute to the accuracy of the production process but they will not have direct access to the closed shop environment. They cannot adversely influence the integrity of the closed shop environment, other than by inadequate performance of their adjustment functions and tasks.

Management will have timely information about the company and the position of the company in relation to the outside world so that it can assess the desired performance of corporate operations in its entirety. Detailed reporting concerning the way in which responsibilities are carried out by the closed shop environment is required. These reports will be from the perspective of the processes and from the perspective of the corporate operations (current and forecast expenditure and income). They will offer management the possibility of intervening in good time by applying adaptive control measures to the system.

4 SUMMARY AND CONCLUSIONS

A number of myths concerning a sound structure for the organization of business tasks within a company must be dealt with.
Human input does not need to be verified for the accuracy of the output to be considered reliable. If the company makes a third party contractually responsible for the input and has sufficient resources in-house to be able to demonstrate that the data cannot be distorted within the company, such verification is not necessary. Check sums are not needed to ascertain the integrity of automated processes in good time. Check sums are usually ineffective in a real time environment. The preventative control measures must be sufficient.
Technical systems management, and the functions for developing systems and for troubleshooting, may not be given access to the closed shop environment. Their support must be absolutely unnecessary. If this position is taken, the required stability of the closed shop environment is achievable. The separation of responsibility for the computer center from the other tasks is a precondition to guarantee the necessary segregation of duties between development (and/or modifications in accepted systems) and the use of these systems. Comparing the individual outputs from systems with records on paper is an ineffective and extremely inefficient way of obtaining the required confidence with regard to the accuracy of the processing when the company works exclusively with automated processes.

It is becoming clear that companies have to pay much more attention than before to achieving professional automated support of the business. An important requirement for this is the use of a clarification of processes, data and the internal organization according to their risks to the company in terms of the privacy of data, integrity and the overall continuity of the company.
Measures to manage the technical infrastructure of the automated systems must take into account efficient and effective control procedures for the various classes of systems and environments. The management of the architecture of the information systems must be designed in such a way that the company can guarantee the presence of the required controls on the integrity of information

processing and on the links between the information systems. The computer center functions must be automated as fully as possible so that the operation of the technical infrastructure is controllable and human intervention is only required in very exceptional cases.

The audit of a highly automated environment so that the company, the auditor and society can rely on these systems has become a requirement. An auditing body specializing in the field of auditing, automation and IT which is impartial and independent of the decisions regarding the design of the automated systems (both technical and application systems) will be used. Such an auditor can issue statements to society on the adequacy of compliance with measures required by law, such as the privacy legislation and the computer crime act. Social dependency on systems managed by certain computer centers will lead to the need to issue statements concerning the adequacy of the organizational design of these automated systems and of the computer centers.

This article deals with the growing influence of automation on the current organization of companies. In particular the article is concerned with the implications of this growing influence on the control structures of a company. If considers ‘IT’ as a 'partner' in the business operations and not merely a supporting tool for activities to be performed by human beings. It was stated that the automation has to be designed very tightly and in accordance with rigorous procedures so that the 'partnership' can be achieved properly. The growing influence of automation has also had an effect on the development of IT auditing. The knowledge and know-how required for advising a company about the best way to shape this partnership calls for auditors with an affinity for and experience with IT and the management of change. The adequacy of the design for use of IT must be assessed in relation to the overall internal organization and corporate objectives.

It is unfortunate that a growing number of technologies are being developed which do not meet the requirements for rapid and effective use in the closed shop environment described in this article. The lack of attention to the development of interfacing techniques and protocols for safe communication between IT environments with different security levels also slows down the achievement of a more complete use of IT within modern businesses.

References:

IT Auditing, an object-oriented approach. Chapter 4. Delwel Publishers, The Hague, ISBN 9061557763. 1996.

'Electronische snelweg' (Information Superhighway). M.E. van Biene-Hershey and N.H.J. Thuys. *Auditing changes and changing auditing. Anniversary symposium 16 June 1995*. Tilburg University Press, ISBN 90-361-9946-8. 1996.

'Security more important than ever! 'M.E. van Biene-Hershey, **Bewaar Me, Liber amoricorum voor Prof. dr. I.S. Herschberg,** ISBN 90-901-1372-X, 1998.